

2013 Cryptologic History Symposium  
*‘Technological Change and Cryptology:  
Meeting the Historical Challenges’*

DAY ONE: THURSDAY, 17 October 2013

0700-0800—Morning Reception 1 (Registration Opens)

0800-0830—Welcoming Remarks and Opening Address (A)

Moderator: Dr. William J. Williams, Chief, Center for  
Cryptologic History (CCH)

KEYNOTE 1: John C. (Chris) Inglis, Deputy Director,  
National Security Agency (NSA)

0830-0845—BREAK 1

0845-1015—PANEL 1: “Turing at a Century: Revelations and  
Legacies” (A)

Moderator: Dr. David Kahn, Independent Scholar

Dr. David Hatch, CCH

“Turing in the Context of History”

Dr. Craig Bauer, York College of Pennsylvania

“Alan Turing’s Work on Voice Encryption”

Dr. Sandy Zabell, Northwestern University

“Commentary on Alan M. Turing: The Applications of Probability to  
Cryptography”

1015-1045—BREAK 2

1045-1200—(concurrent sessions)

PANEL 2A— “Intelligence Preparations for the Next War” (A)

Moderator: Betsy Rohaly Smoot, CCH

John F. Dooley, Knox College

“SIS and Cipher Machines, 1930-1940”

Dr. Timothy S. Wolters, Iowa State University

“Mechanical Encryption in the U.S. Navy, 1917-1940”

Colin Burke, University of Maryland at Baltimore County

“What OSS Black Chamber? What Yardley? What ‘Dr.’ Friedman? Ah,  
Grombach?: The Effort to Launch a World War II Black Chamber”

Dr. Mark Stout, Johns Hopkins University

“Herbert Yardley’s (Unkown) Wartime Career”

PANEL 2B – “Cipher Systems and Methods” (C1)

Moderator: Barry Carleen, CCH

Tom Vidar Olsen, Norwegian National Security Authority

“Holvand and the Invention of the Rotor Machine, 1904-1910”

Ralph Simpson, Cisco Systems (ret.)

“The Invention of the One-time Pad”

Dr. Chris Christensen, Northern Kentucky University

“Hall’s Weights and Shinn Weights”

Dr. Steven M. Bellovin, Columbia University

“The One-time Pad and the Index of Coincidence”

1200-1300 —LUNCHEON 1 (M)

Moderator: Dr. William J. Williams, Chief, CCH

KEYNOTE 2: Carol B. Davis, CCH (ret.)

“Russian Plaintext: An Early Cold War COMINT Success”

1300-1330 —DEMONSTRATION 1: “Cryptology as Musical Entertainment” (A)

Moderator: Dr. David Hatch, CCH

The Parkway Chorale

“A Musical Showcase of Cryptology”

1330-1415 —(concurrent sessions)

DEMONSTRATION 2: “Research in Progress” (A)

Moderator: Dr. Timothy J. Mucklow, CCH (ret.)

Whitfield Diffie, Dr.Sc., Sun Microsystems

“The ECM Mark I: How It Worked”

PANEL 3 – “Cryptology in the Ancient World” (C1)

Moderator: Greg Nedved, CCH

Ralph D. Sawyer, University of Calgary

“Clandestine Communications in Historic China”

Dr. Frank Russell, University of Transylvania

“Cryptography in Ancient Greece: Information Security or Recognition Device?”

1415-1445 – BREAK 3

1445-1600 —PANEL 4: “Evolution of NSA’s Cutting Edge” (A)

Moderator: Brian Snow, Information Assurance Directorate (ret.)

David P. Cooley, CCH

“Voices of SIGINT Technology: Reflections from NSA’s Early Technical Leaders”

Jim Boone, Research & Engineering (ret.)

“Applying Advanced Technology to Cryptologic Systems: Some Special Management Challenges”

Dr. John O’Hara, Office of Advanced Research (ret.)

“Analog Recording of Telemetry Signals Prior to the Advent of Digital Processing”

1600-1615 – BREAK 4

1615-1730 – PLENARY 1: “Roundtable on Cyber History” (A)

Moderator: Dr. Michael Warner, U.S. Cyber Command

Dr. Abraham Wagner, Columbia University

Jason Healey, the Atlantic Council

Dr. Roger Schell, AESEC Corporation

Sean Kanuck, National Intelligence Officer for Cyber

2013 Cryptologic History Symposium  
*‘Technological Change and Cryptology:  
Meeting the Historical Challenges’*

DAY TWO: FRIDAY, 18 October 2013

0700-0800—Morning Reception 2 (Registration Continues)

0800-0915—(concurrent sessions)

PANEL 5A – “Cryptology & the Advent of New Technologies” (A)

Moderator: Dr. William J. Williams, Chief, CCH

Dr. William Casselman, University of California - Berkeley

“Technical Aspects of the Polish Decryption of Enigma”

Paul E. Ceruzzi, National Air & Space Museum

“The Culture of Precise Positioning: Origins and Applications of GPS Technology”

Dr. Niels Jorgensen, Roskilde University

“Open Encryption Technology and Social Movements”

Elonka Dunin, Simutronics

“Origins and Evolution of Geocaching and Cryptology”

PANEL 5B – “Wartime Intelligence Operations” (C1)

Moderator: Greg Nedved, CCH

Dr. Chris Christensen, Northern Kentucky University

“The U.S. Navy’s Attack on JN-25”

Michael W. Pfarr, Jr., Department of Defense

“Richard Sorge and the Book Cipher”

Dr. Steve Huffman, Department of Defense

Codetalkers and Codetalking: The Rest of the Story”

Steven Wagner, University of Oxford

“ ‘Blowing the Source’: Britain’s Use of SIGINT in Palestine, 1933-1947”

DEMONSTRATION 2: “Bletchley Park Celebrated” (C2)

Moderator: Dr. David H. Hamer, National Cryptologic Museum Foundation

Benjamin Gatti and Bob Weiss, Password Crackers, Inc.

“Breaking the Enigma: A Live Demonstration”

CWO George Keller, U.S. Navy Reserve (ret.)

“Bletchley Park Revisited: A Photographic Essay”

0915-0945—BREAK 5

0945-1045 – (concurrent sessions)

PANEL 6A: “In War’s Aftermath: Cryptology and the Early Cold War” (A)

Moderator: Dr. David Hatch, CCH

Dr. Thomas Johnson, CCH (ret.)

“American Cryptology during the Cold War”

Robert J. Hanyok, CCH (ret.)

“On the Edge of Tomorrow’s War: WWII COMINT Confronts Ballistic Missiles and Atomic Weapons”

PANEL 6B – “COMINT and the Civil War” (C1)

Moderator: Patrick Weadon, National Cryptologic Museum

Jennifer Wilcox, National Cryptologic Museum

“Signaling the Civil War: The Rise of Two Key Technologies, 1861-1865”

Tim Carver, Trine University

“Analysis of Espionage: Rose Greenhow’s Cipher Examined”

1045-1100 —BREAK 6

1100-1215 —(concurrent sessions)

PANEL 7A: “Legacies of the Great War & the Interwar Years” (A)

Moderator: Dr. Mark Stout, Johns Hopkins University

Dr. Laurence Lyons, British Aerospace (ret.) and

Carl J. Bobrow, National Air & Space Museum

“WWI and the Paradigm Shift in Wireless Communications”

Betsy Rohaly Smoot, CCH

“Technology and Radio Intercept: The Site at Houlton, Maine, 1918-1920”

Dr. John Ferris, University of Calgary

“Commercial Codes of World Banking, 1916-1942”

Dr. Victor Madeira, U.S. European Command

“All the King’s (P)Russians: the Vetterleins and British Cryptography, 1918-1944”

PANEL 7B – “SIGINT and the Vietnam War Era” (C1)

Moderator: David P. Cooley, CCH

Theresa Monserrat, University of Southern Mississippi

““American Prestige Has Suffered”: Reactions to the *PUEBLO* Crisis”

Scott Laidig, U.S. Marine Corps (ret.)

“SIGINT Marines: Preparing the Marine Corps for Vietnam, 1954-1968”

Tom Glenn, Department of Defense (ret.)

“Recollections of the Fall of Saigon”

PANEL 7C: “Historical Codes and Ciphers” (C2)

Moderator: Greg Nedved, CCH

Dr. Joel Freeman, Independent Scholar

“Exactly How the Rosetta Stone was Cracked”

Todd Mateer, Department of Defense

“Cryptanalysis of Beale Cipher Number Two”

Dr. Nicholas Gessler, Duke University

“The Aspinwall Cypher of the Revolutionary War”

1215-1315—LUNCHEON 2 (M)

Moderator: Dr. William J. Williams, Chief, CCH

KEYNOTE 3: Dr. George R. Cotter, Chief Information Officer,  
NSA (ret.)

“Mission, Technologies, and Heroes”

1315-1430—(concurrent sessions)

PANEL 8A – “Cryptology in Life and Literature” (A)

Moderator: Dr. David Hatch, CCH

Dr. Gerhard F. Strasser, The Pennsylvania State University

“‘Encoded’ Communication with Ladies in a Turkish Harem,  
17<sup>th</sup> Century Style!”

Dr. Benedek Lang, Budapest University of Technology

“Shame, Sex, and Alcohol: Ciphers in the Context of Everyday Practices of  
Secrecy in Early Modern Times”

Erin Higgins, Department of Defense

“Examples of Steganography in de Vigenère’s *Traite des Chiffres*”

Klaus Schmeh, Independent Scholar

“Encrypted Books: Why Some Secrets Fill Hundreds of Pages”

PANEL 8B – “East European COMINT during World War II” (C1)

Moderator: Dr. Thomas Johnson, CCH (ret.)

Dr. Jerca Vodusek Staric, University of Maribor

“The Emergence of Partisan Espionage and Counterintelligence during WWII”

Dr. Lavinia Ciungu, University of Iowa

“Romania’s Wartime Cryptologic Activities”

Dr. Laszlo Ritter, Hungarian Academy of Sciences

“A Little-Known Counterintelligence Success Story: SIGINT’s Role in Axis  
Operations against Allied Intelligence Networks in Central Europe”

PANEL 8C – “New Voices in Cryptologic History” (C2)

Moderator: Dr. Kent Sieg, CCH

Richard Greeley, Department of Defense  
“SIGINT in the Spanish-American War”  
Capt Kelly Elizabeth Atkinson, U.S. Air Force  
“Examining the U.S. Intelligence Failures in Detecting the Attack  
on Pearl Harbor”  
Jared Antrobus, Northern Kentucky University  
“Alignment of JN-25 Enciphered Groups and Additives  
Jeffrey Berkey, Independent Scholar  
“Elizebeth Smith Friedman: Cryptologic Pioneer”

1430-1500—BREAK 7

1500-1630—PLENARY 2: “A Technological Advantage:  
Perspectives on Information & Communications Systems  
Development” (A)  
Moderator: Ronald J. Lucas, CCH  
Dr. Nancy Welker, Operational Test Authority  
Dr. Fernand Bedard, Laboratory for Physical Sciences  
Dan Both, Microelectronics Solutions  
Dr. Tony Chernoske, Special Processing Laboratory (ret.)  
Baron Mills, High Performance Computing Technology

[Legend for session location – A=Auditorium, C1=Classroom 1, C2=Classroom 2, M=Mezzanine]